

博士论文

基于快速公钥签名的自组网QoS多播路由认证

杨铭熙, 李腊元

(武汉理工大学计算机学院, 武汉 430070)

收稿日期 修回日期 网络版发布日期 2007-11-26 接受日期

**摘要** 提出了一个新的具备安全功能的Ad hoc网多QoS约束的多播路由协议NSQMRAN。该协议采用新型公钥签名算法NTRUSign作为密码机制为路由报文签名, 加强了安全性。NSQMRAN为Ad hoc网QoS多播路由协议增加了源认证机制, 从而提供了QoS多播路由报文的来源真实性、数据完整性和抗否认等安全服务以抵御恶意节点的攻击。基于NS2的仿真结果表明, 在Ad hoc网中, 与采用RSA公钥算法的协议相比, 采用NTRUSign的NSQMRAN协议网络性能较好, 产生较少的端到端延迟。

**关键词** [QoS](#); [多播](#); [公钥](#); [NTRUSign](#); [认证](#)

**分类号** [TP309](#)

**DOI:**

对应的英文版文章: [23-01b](#)

通讯作者:

作者个人主页: [杨铭熙](#); [李腊元](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (313KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [参考文献\[PDF\]](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“QoS; 多播; 公钥; NTRUSign; 认证”的 相关文章](#)

▶ 本文作者相关文章

· [杨铭熙](#)

· [李腊元](#)